

Frobenius Distributions

Edgar Costa (MIT)

Simons Collab. on Arithmetic Geometry, Number Theory, and Computation

February 19th, 2020

University of California San Diego

Slides available at edgarcosta.org under Research

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
 - factorization of $f_p(x) \rightsquigarrow$
 - factorization of $f(x)$
 - e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
 - factorization of p in $\mathbb{Q}[x]/f(x)$

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
 - factorization of $f_p(x) \rightsquigarrow$
 - factorization of $f(x)$
 - e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
 - factorization of p in $\mathbb{Q}[x]/f(x)$
- What can we say about $f_p(x)$ for arbitrary p ?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
 - factorization of $f_p(x) \rightsquigarrow$
 - factorization of $f(x)$
 - e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
 - factorization of p in $\mathbb{Q}[x]/f(x)$
 - What can we say about $f_p(x)$ for arbitrary p ?
 - For $\deg f = 2$, quadratic reciprocity gives us that

$$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

depending only on $p \bmod \Delta(f)$.

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
 - factorization of $f_p(x) \rightsquigarrow$
 - factorization of $f(x)$
 - e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
 - factorization of p in $\mathbb{Q}[x]/f(x)$
 - What can we say about $f_p(x)$ for arbitrary p ?
 - For $\deg f = 2$, quadratic reciprocity gives us that

$$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

depending only on $p \bmod \Delta(f)$.

- What about for higher degrees?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
 - factorization of $f_p(x) \rightsquigarrow$
 - factorization of $f(x)$
 - e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
 - factorization of p in $\mathbb{Q}[x]/f(x)$
 - What can we say about $f_p(x)$ for arbitrary p ?
 - For $\deg f = 2$, quadratic reciprocity gives us that

$$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

depending only on $p \bmod \Delta(f)$.

- What about for higher degrees?

\rightsquigarrow studying the **statistical** properties $N_f(p)$.

Example: Cubic polynomials

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \text{ fixes } i \text{ roots}),$$

Example: Cubic polynomials

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \text{ fixes } i \text{ roots}),$$

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2}) (x - \sqrt[3]{2}e^{2\pi i/3}) (x - \sqrt[3]{2}e^{4\pi i/3})$$

$$\text{Prob}(N_f(p) = k) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases}$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1) (x - \alpha_2) (x - \alpha_3)$$

$$\text{Prob}(N_g(p) = k) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases}$$

Example: Cubic polynomials

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \text{ fixes } i \text{ roots}),$$

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2}) (x - \sqrt[3]{2}e^{2\pi i/3}) (x - \sqrt[3]{2}e^{4\pi i/3})$$

$$\text{Prob}(N_f(p) = k) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(f) = S_3$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1) (x - \alpha_2) (x - \alpha_3)$$

$$\text{Prob}(N_g(p) = k) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(g) = \mathbb{Z}/3\mathbb{Z}$$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p ?

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p ?
- Given $\#E_p$ for many p , what can we say about E ?

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p ?
- Given $\#E_p$ for many p , what can we say about E ?

\rightsquigarrow studying the **statistical** properties $\#E_p$.

Hasse's bound

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Hasse's bound

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Alternatively, we could also have written the formula above as

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Hasse's bound

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Alternatively, we could also have written the formula above as

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

or

$\#E_p = L(1)$, where

$$L(T) = 1 - a_p T + pT^2 = \det(1 - T \text{Frob}_p | H^1(E))$$

Hasse's bound

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Alternatively, we could also have written the formula above as

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

or

$\#E_p = L(1)$, where

$$L(T) = 1 - a_p T + pT^2 = \det(1 - T \text{Frob}_p | H^1(E))$$

Question

What can we say about the error term a_p/\sqrt{p} as $p \rightarrow \infty$?

Two types of elliptic curves

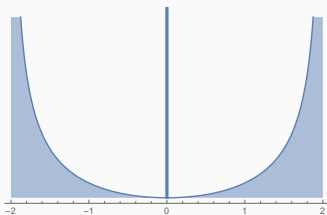
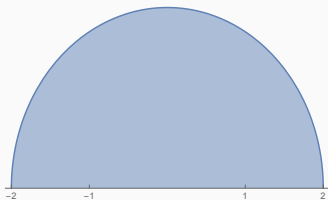
$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}



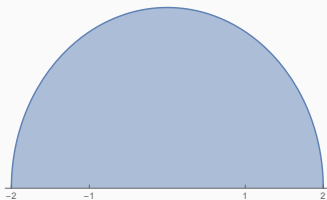
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

non-CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$$



CM

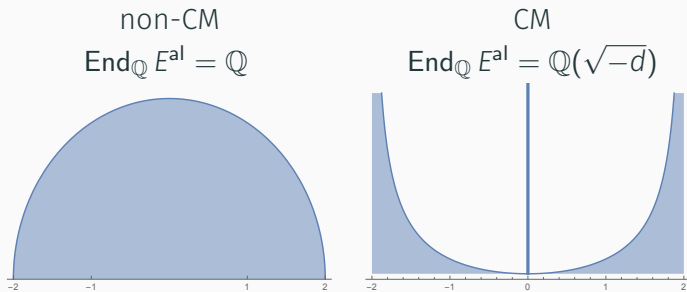
$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-d})$$



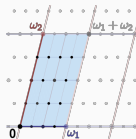
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}



Over \mathbb{C} an elliptic curve E is a torus
 $E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 =$
and we have $\text{End } E^{\text{al}} = \text{End } \Lambda$



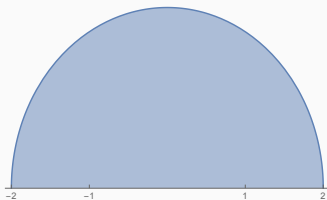
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

non-CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$$



CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-d})$$



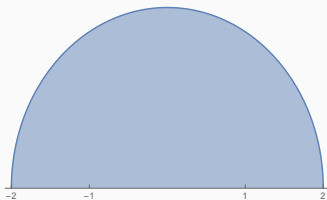
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

non-CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$$



$$\text{Prob}(a_p = 0) \stackrel{?}{\sim} 1/\sqrt{p}$$

CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-d})$$



$$\text{Prob}(a_p = 0) = 1/2$$

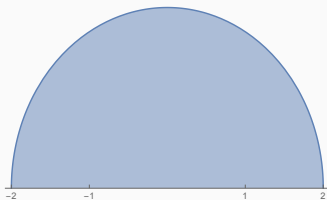
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

non-CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$$



$$\text{Prob}(a_p = 0) \stackrel{?}{\sim} 1/\sqrt{p}$$

CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-d})$$



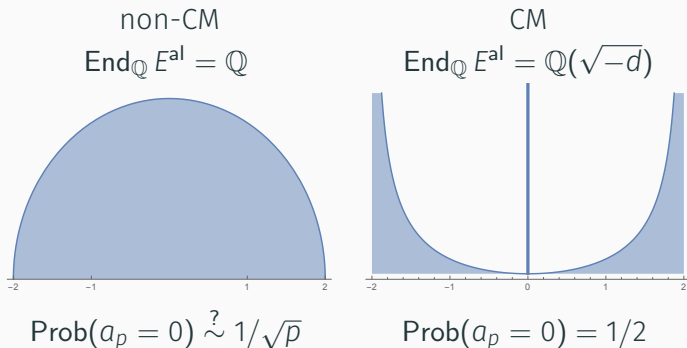
$$\text{Prob}(a_p = 0) = 1/2$$

$$a_p = 0 \iff \mathbb{Q}(\text{Frob}_p) \subsetneq \text{End}_{\mathbb{Q}} E_p^{\text{al}}$$

Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for a_p/\sqrt{p}

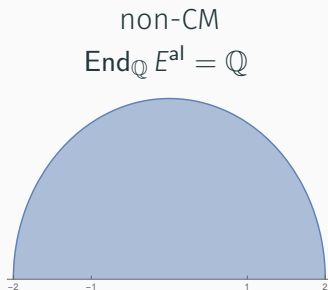


$$\begin{aligned} a_p = 0 &\iff \mathbb{Q}(\text{Frob}_p) \subsetneq \text{End}_{\mathbb{Q}} E_p^{\text{al}} \\ &\iff \dim \text{End}_{\mathbb{Q}} E_p^{\text{al}} > 2 \end{aligned}$$

Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \text{Tr Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

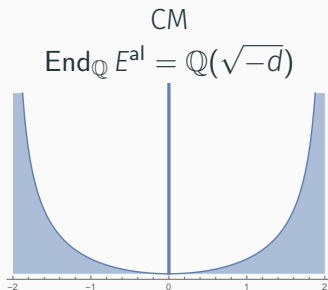
There are two limiting distributions for a_p/\sqrt{p}



$$\text{Prob}(a_p = 0) \stackrel{?}{\sim} 1/\sqrt{p}$$

$$a_p = 0 \iff \mathbb{Q}(\text{Frob}_p) \subsetneq \text{End}_{\mathbb{Q}} E_p^{\text{al}}$$

$$\iff \dim \text{End}_{\mathbb{Q}} E_p^{\text{al}} > 2 = \min_q \dim \text{End}_{\mathbb{Q}} E_q^{\text{al}}$$

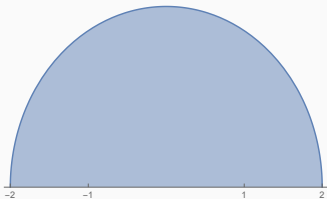


$$\text{Prob}(a_p = 0) = 1/2$$

How to distinguish between the two types?

non-CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$$



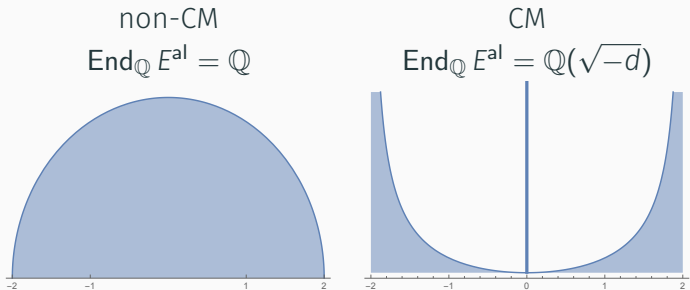
CM

$$\text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-d})$$



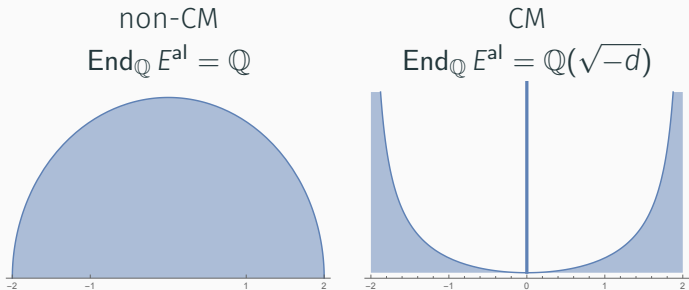
- $\text{End}_{\mathbb{Q}} E^{\text{al}} \hookrightarrow \text{End}_{\mathbb{Q}} E_p^{\text{al}} \hookrightarrow \mathbb{Q}(\text{Frob}_p)$
- $a_p \neq 0 \iff \text{End}_{\mathbb{Q}} E_p^{\text{al}}$ is a quadratic field

How to distinguish between the two types?



- $\text{End}_{\mathbb{Q}} E^{\text{al}} \hookrightarrow \text{End}_{\mathbb{Q}} E_p^{\text{al}} \hookrightarrow \mathbb{Q}(\text{Frob}_p)$
- $a_p \neq 0 \iff \text{End}_{\mathbb{Q}} E_p^{\text{al}}$ is a quadratic field
- If E has CM, then
$$a_p \equiv 0 \pmod{p} \iff p \text{ inert or ramified in } \mathbb{Q}(\sqrt{-d})$$
$$\iff \text{End}_{\mathbb{Q}} E^{\text{al}} \not\cong \text{End}_{\mathbb{Q}} E_p^{\text{al}}$$

How to distinguish between the two types?



- $\text{End}_{\mathbb{Q}} E^{\text{al}} \hookrightarrow \text{End}_{\mathbb{Q}} E_p^{\text{al}} \hookrightarrow \mathbb{Q}(\text{Frob}_p)$
- $a_p \neq 0 \iff \text{End}_{\mathbb{Q}} E_p^{\text{al}}$ is a quadratic field
- If E has CM, then
$$a_p \equiv 0 \pmod{p} \iff p \text{ inert or ramified in } \mathbb{Q}(\sqrt{-d})$$
$$\iff \text{End}_{\mathbb{Q}} E^{\text{al}} \not\cong \text{End}_{\mathbb{Q}} E_p^{\text{al}}$$
- If E is non-CM, then $\text{End}_{\mathbb{Q}} E_p^{\text{al}} \cap \text{End}_{\mathbb{Q}} E_q^{\text{al}} \simeq \mathbb{Q}$ with prob. 1 and we expect $\text{Prob}(a_p \equiv 0 \pmod{p}) \sim 1/\sqrt{p}$

Examples

$$E : y^2 + y = x^3 - x^2 - 10x - 20 \quad (11.a2)$$

- $\text{End}_{\mathbb{Q}} E_2^{\text{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\text{End}_{\mathbb{Q}} E_3^{\text{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$

Examples

$$E : y^2 + y = x^3 - x^2 - 10x - 20 \text{ (11.a2)}$$

- $\text{End}_{\mathbb{Q}} E_2^{\text{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\text{End}_{\mathbb{Q}} E_3^{\text{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}$

$$E : y^2 + y = x^3 - 7 \text{ (27.a2)}$$

- $p = 2 \pmod{3} \Rightarrow a_p = 0 \Rightarrow \text{End}_{\mathbb{Q}} E_p^{\text{al}}$ is a Quaternion algebra
- $p = 1 \pmod{3} \Rightarrow \text{End}_{\mathbb{Q}} E_p^{\text{al}} \simeq \mathbb{Q}(\sqrt{-3})$
- $\rightsquigarrow \text{End}_{\mathbb{Q}} E^{\text{al}} = \mathbb{Q}(\sqrt{-3})$

Genus 2 curves/Abelian surfaces

$$A := \text{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

Genus 2 curves/Abelian surfaces

$$A := \text{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\text{End}_{\mathbb{R}} A^{\text{al}}$
square of CM elliptic curve	$M_2(\mathbb{C})$
<ul style="list-style-type: none">• QM abelian surface• square of non-CM elliptic curve	$M_2(\mathbb{R})$
<ul style="list-style-type: none">• CM abelian surface• product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
<ul style="list-style-type: none">• RM abelian surface• product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	\mathbb{R}

Genus 2 curves/Abelian surfaces

$$A := \text{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\text{End}_{\mathbb{R}} A^{\text{al}}$
square of CM elliptic curve	$M_2(\mathbb{C})$
<ul style="list-style-type: none">• QM abelian surface• square of non-CM elliptic curve	$M_2(\mathbb{R})$
<ul style="list-style-type: none">• CM abelian surface• product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
<ul style="list-style-type: none">• RM abelian surface• product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	\mathbb{R}

Can we distinguish between these by looking at $A \bmod p$?

Zeta functions and Frobenius polynomials

- C/\mathbb{Q} a nice curve of genus g
- $A := \text{Jac}(C)$
- p a prime of good reduction

$$Z_p(T) := \exp \left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r}) T^r / r \right) \in \mathbb{Q}(t)$$

Zeta functions and Frobenius polynomials

- C/\mathbb{Q} a nice curve of genus g
- $A := \text{Jac}(C)$
- p a prime of good reduction

$$Z_p(T) := \exp \left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r}) T^r / r \right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T) = 2g$ and

$$L_p(T) = \det(1 - t \text{Frob}_p | H^1(C)) = \det(1 - t \text{Frob}_p | H^1(A))$$

Zeta functions and Frobenius polynomials

- C/\mathbb{Q} a nice curve of genus g
- $A := \text{Jac}(C)$
- p a prime of good reduction

$$Z_p(T) := \exp \left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r}) T^r / r \right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T) = 2g$ and

$$L_p(T) = \det(1 - t \text{Frob}_p | H^1(C)) = \det(1 - t \text{Frob}_p | H^1(A))$$

- $g = 1 \rightsquigarrow L_p(T) = 1 - a_p T + pT^2$
- $g = 2 \rightsquigarrow L_p(T) = 1 - a_{p,1}T + a_{p,2}T^2 - a_{p,1}pT^3 + p^2T^4$

$L_p(T)$ gives us a lot of information about $A_p := A \bmod p$

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over \mathbb{F}_q , given

$$\det(1 - t \text{Frob} | H^1(A)),$$

we may compute

$$\text{rk End}(A_{\mathbb{F}_{q^r}}), \quad \forall r \geq 1$$

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over \mathbb{F}_q , given

$$\det(1 - t \text{Frob} | H^1(A)),$$

we may compute

$$\text{rk End}(A_{\mathbb{F}_{q^r}}), \quad \forall r \geq 1$$

Honda–Tate theory \implies gives us $\text{End}_{\mathbb{Q}}(A_{\mathbb{F}_{q^r}})$ up to isomorphism

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over \mathbb{F}_q , given

$$\det(1 - t \text{Frob} | H^1(A)),$$

we may compute

$$\text{rk End}(A_{\mathbb{F}_{q^r}}), \quad \forall r \geq 1$$

Honda–Tate theory \implies gives us $\text{End}_{\mathbb{Q}}(A_{\mathbb{F}_{q^r}})$ up to isomorphism

Example

If $L_5(T) = 1 - 2T^2 + 25T^4$, then:

- all endomorphisms are defined over \mathbb{F}_{25} , and
- $A_{\mathbb{F}_{25}}$ is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over \mathbb{F}_{25}
- $\det(1 - T \text{Frob}_5^2 | H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over \mathbb{F}_{25} is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over \mathbb{F}_{25}
- $\det(1 - T \text{Frob}_5^2 | H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over \mathbb{F}_{25} is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over \mathbb{F}_{49}
- $\det(1 - T \text{Frob}_7^2 | H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over \mathbb{F}_{49} is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A_7^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over \mathbb{F}_{25}
- $\det(1 - T \text{Frob}_5^2 | H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over \mathbb{F}_{25} is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over \mathbb{F}_{49}
- $\det(1 - T \text{Frob}_7^2 | H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over \mathbb{F}_{49} is isogenous to a square of an elliptic curve
- $\text{End}_{\mathbb{Q}} A_7^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

$$\Rightarrow \text{End}_{\mathbb{R}} A^{\text{al}} \neq M_2(\mathbb{C})$$

Same L_p , different approach

We could have looked at the Néron–Severi lattice.

$$\mathrm{NS}(A^{\mathrm{al}}) \hookrightarrow \mathrm{NS}(A_p^{\mathrm{al}})$$

- $\mathrm{rk} \mathrm{NS}(A^{\mathrm{al}}) \in \{1, 2, 3, 4\}$
- $\mathrm{rk} \mathrm{NS}(A_p^{\mathrm{al}}) \in \{2, 4, 6\}$

Example

- $\mathrm{rk} \mathrm{NS}(A_5^{\mathrm{al}}) = \mathrm{rk} \mathrm{NS}(A_7^{\mathrm{al}}) = 4$
 - $\mathrm{disc} \mathrm{NS}(A_5^{\mathrm{al}}) = -6 \pmod{\mathbb{Q}^{\times 2}}$
 - $\mathrm{disc} \mathrm{NS}(A_7^{\mathrm{al}}) = -10 \pmod{\mathbb{Q}^{\times 2}}$
- $\Rightarrow \mathrm{rk} \mathrm{NS}(A^{\mathrm{al}}) \leq 3$

Fact

By a theorem of Charles, we know that at some point this method will attain a tight upper bound for $\mathrm{rk} \mathrm{NS}(A^{\mathrm{al}})$.

Real endomorphisms algebras and Picard numbers

Abelian surface	$\text{End}_{\mathbb{R}} A^{\text{al}}$	$\text{rk NS}(A^{\text{al}})$
square of CM elliptic curve	$M_2(\mathbb{C})$	4
• QM abelian surface	$M_2(\mathbb{R})$	3
• square of non-CM elliptic curve		
• CM abelian surface	$\mathbb{C} \times \mathbb{C}$	2
• product of CM elliptic curves		
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	2
• RM abelian surface	$\mathbb{R} \times \mathbb{R}$	2
• product of non-CM elliptic curves		
generic abelian surface	\mathbb{R}	1

Higher genus

Let K be a numberfield such that $\text{End } A_K = \text{End } A^{\text{al}}$

Higher genus

Let K be a numberfield such that $\text{End } A_K = \text{End } A^{\text{al}}$, then

- $A_K \sim \prod_{i=1}^t A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \text{End}_{\mathbb{Q}} A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\dim_{L_i} B_i = e_i^2$,
- $\text{End}_{\mathbb{Q}} A_K = \prod_{i=1}^t M_{n_i}(B_i)$

Higher genus

Let K be a numberfield such that $\text{End } A_K = \text{End } A^{\text{al}}$, then

- $A_K \sim \prod_{i=1}^t A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \text{End}_{\mathbb{Q}} A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\dim_{L_i} B_i = e_i^2$,
- $\text{End}_{\mathbb{Q}} A_K = \prod_{i=1}^t M_{n_i}(B_i)$

Theorem (C-Mascot-Sijsling-Voight, C-Lombardo-Voight)

If Mumford-Tate conjecture holds for A , then we can compute

- t
- $\{(e_i n_i, n_i \dim A_i)\}_{i=1}^t$
- L_i

This is practical and its done by counting points (=computing L_p)

Real endomorphisms algebras, $\{e_i n_i, n_i \dim A_i\}_{i=1}^t$, and $\dim L_i$

Abelian surface	$\text{End}_{\mathbb{R}} A^{\text{al}}$	tuples	$\dim L_i$
square of CM elliptic crv	$M_2(\mathbb{C})$	$\{(2, 2)\}$	2
• QM abelian surface	$M_2(\mathbb{R})$	$\{(2, 2)\}$	1
• square of non-CM elliptic crv			
• CM abelian surface	$\mathbb{C} \times \mathbb{C}$	$\{(1, 2)\}$	4
• product of CM elliptic crv			$\{(1, 1), (1, 1)\}$
CM \times non-CM elliptic crvs	$\mathbb{C} \times \mathbb{R}$	$\{(1, 1), (1, 1)\}$	2, 1
• RM abelian surface	$\mathbb{R} \times \mathbb{R}$	$\{(1, 2)\}$	2
• prod. of non-CM elliptic crv			$\{(1, 1), (1, 1)\}$
generic abelian surface	\mathbb{R}	$\{(1, 1)\}$	1

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

- $\text{End}_{\mathbb{Q}} A_3^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \text{End}_{\mathbb{R}} A^{\text{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \text{End}_{\mathbb{Q}} A^{\text{al}}$ and assume that B is a quaternion algr.
Can we guess $\text{disc } B$?

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

- $\text{End}_{\mathbb{Q}} A_3^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \text{End}_{\mathbb{R}} A^{\text{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \text{End}_{\mathbb{Q}} A^{\text{al}}$ and assume that B is a quaternion algr.
Can we guess $\text{disc } B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\text{Frob}_p)$

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

- $\text{End}_{\mathbb{Q}} A_3^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \text{End}_{\mathbb{R}} A^{\text{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \text{End}_{\mathbb{Q}} A^{\text{al}}$ and assume that B is a quaternion algr.
Can we guess $\text{disc } B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\text{Frob}_{\ell})$

- $5, 13, 17 \nmid \text{disc } B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \text{disc } B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd).

Example continued

$$A = \text{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

- $\text{End}_{\mathbb{Q}} A_3^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\text{End}_{\mathbb{Q}} A_5^{\text{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \text{End}_{\mathbb{R}} A^{\text{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \text{End}_{\mathbb{Q}} A^{\text{al}}$ and assume that B is a quaternion algr.
Can we guess $\text{disc } B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\text{Frob}_{\ell})$

- $5, 13, 17 \nmid \text{disc } B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \text{disc } B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd).
Indeed, $\text{disc } B = 6$.

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

They may arise in many ways:

- smooth quartic surfaces in \mathbb{P}^3

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of \mathbb{P}^2 branched over a sextic curve

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

They may arise in many ways:

- smooth quartic surfaces in \mathbb{P}^3

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of \mathbb{P}^2 branched over a sextic curve

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

Can we play similar game as before?

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

They may arise in many ways:

- smooth quartic surfaces in \mathbb{P}^3

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of \mathbb{P}^2 branched over a sextic curve

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

Can we play similar game as before?

In this case, instead of studying $\#X_p$ or Tr Frob_p we study

$$p \longmapsto \text{rk NS } X_p^{\text{al}} \in \{2, 4, \dots, 22\}$$

K3 Surfaces

X/\mathbb{Q} a K3 surface

$$p \longmapsto \text{rk NS } X_p^{\text{al}} \in \{2, 4, \dots, 22\}$$

This is analogous to studying:

$$p \longmapsto \text{rk End } E_p^{\text{al}} \in \{2, 4\}$$

K3 Surfaces

X/\mathbb{Q} a K3 surface

$$p \longmapsto \text{rk NS } X_p^{\text{al}} \in \{2, 4, \dots, 22\}$$

This is analogous to studying:

$$p \longmapsto \text{rk End } E_p^{\text{al}} \in \{2, 4\}$$

Recall that:

- $\text{rk End } E_p^{\text{al}} = 4 \iff a_p = 0$
- $\text{Prob}(a_p = 0) = \begin{cases} \sim \frac{1}{\sqrt{p}} & \text{if } E \text{ is non-CM (Lang-Trotter)} \\ 1/2 & \text{if } E \text{ has CM by } \mathbb{Q}(\sqrt{-d}) \end{cases}$

In the later case,

$$\{p : a_p = 0\} = \{p : p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d})\}$$

K3 Surfaces

X/\mathbb{Q} a K3 surface

$$\rho \longmapsto \text{rk NS } X_\rho^{\text{al}} \in \{2, 4, \dots, 22\}$$

For an abelian surface A we have:

$$\text{NS}(A)_{\mathbb{Q}} \simeq \{\phi \in \text{End}(A)_{\mathbb{Q}} : \phi^\dagger = \phi\},$$

where \dagger denotes the Rosati involution.

K3 Surfaces

X/\mathbb{Q} a K3 surface

$$p \longmapsto \text{rk NS } X_p^{\text{al}} \in \{2, 4, \dots, 22\}$$

For an abelian surface A we have:

$$\text{NS}(A)_{\mathbb{Q}} \simeq \{\phi \in \text{End}(A)_{\mathbb{Q}} : \phi^{\dagger} = \phi\},$$

where \dagger denotes the Rosati involution. Thus for A/\mathbb{Q} this is equivalent to

$$p \longmapsto \text{rk End}(A_p^{\text{al}})_{\mathbb{Q}}^{\dagger} = \text{rk NS } A_p^{\text{al}} \in \{2, 4, 6\}$$

Now

- $\text{rk NS } A_p^{\text{al}} \geq 4 \iff A_p^{\text{al}} \sim E^2$
- $\text{rk NS } A_p^{\text{al}} = 6 \iff A_p^{\text{al}} \sim E^2, E \text{ supersingular, i.e., } a_p = 0$

Néron–Severi group

- $\text{NS } \bullet = \text{Néron–Severi group of } \bullet \simeq \{\text{curves on } \bullet\} / \sim$
- $\rho(\bullet) = \text{rk NS } \bullet$
- $X_p := X \bmod p$

Néron–Severi group

- $\text{NS } \bullet = \text{Néron–Severi group of } \bullet \simeq \{\text{curves on } \bullet\} / \sim$
- $\rho(\bullet) = \text{rk NS } \bullet$
- $X_p := X \bmod p$

$$\begin{array}{ccccc} X & \longrightarrow & \text{NS } X^{\text{al}} & \longrightarrow & \rho(X^{\text{al}}) & \in \{1, 2, \dots, 20\} \\ \downarrow & & \downarrow & & \uparrow \text{???} & \\ X_p & \longrightarrow & \text{NS } X_p^{\text{al}} & \longrightarrow & \rho(X_p^{\text{al}}) & \in \{2, 4, \dots, 22\} \end{array}$$

Néron–Severi group

- $\text{NS } \bullet =$ Néron–Severi group of $\bullet \simeq \{\text{curves on } \bullet\} / \sim$
- $\rho(\bullet) = \text{rk NS } \bullet$
- $X_p := X \bmod p$

$$\begin{array}{ccccccc} X & \longrightarrow & \text{NS } X^{\text{al}} & \longrightarrow & \rho(X^{\text{al}}) & \in \{1, 2, \dots, 20\} \\ \downarrow & & \downarrow & & \uparrow \text{ ???} & \\ X_p & \longrightarrow & \text{NS } X_p^{\text{al}} & \longrightarrow & \rho(X_p^{\text{al}}) & \in \{2, 4, \dots, 22\} \end{array}$$

Theorem (Charles)

For infinitely many p we have $\rho(X_p^{\text{al}}) = \min_q \rho(X_q^{\text{al}})$.

The Problem

$$\begin{array}{ccccc} X & \longrightarrow & \text{NS } X^{\text{al}} & \longrightarrow & \rho(X^{\text{al}}) & \in \{1, 2, \dots, 20\} \\ \downarrow & & \downarrow & & \uparrow \text{???} & \\ X_p & \longrightarrow & \text{NS } X_p^{\text{al}} & \longrightarrow & \rho(X_p^{\text{al}}) & \in \{2, 4, \dots, 22\} \end{array}$$

Theorem (Charles)

For infinitely many p we have $\rho(X_p^{\text{al}}) = \min_q \rho(X_q^{\text{al}})$.

What can we say about:

- $\Pi_{\text{jump}}(X) := \{p : \rho(X_p^{\text{al}}) > \min_q \rho(X_q^{\text{al}})\}$

The Problem

$$\begin{array}{ccccc} X & \longrightarrow & \text{NS } X^{\text{al}} & \longrightarrow & \rho(X^{\text{al}}) & \in \{1, 2, \dots, 20\} \\ \downarrow & & \downarrow & & \updownarrow \text{???} & \\ X_p & \longrightarrow & \text{NS } X_p^{\text{al}} & \longrightarrow & \rho(X_p^{\text{al}}) & \in \{2, 4, \dots, 22\} \end{array}$$

Theorem (Charles)

For infinitely many p we have $\rho(X_p^{\text{al}}) = \min_q \rho(X_q^{\text{al}})$.

What can we say about:

- $\Pi_{\text{jump}}(X) := \{p : \rho(X_p^{\text{al}}) > \min_q \rho(X_q^{\text{al}})\}$
- $\gamma(X, B) := \frac{\#\{p \leq B : p \in \Pi_{\text{jump}}(X)\}}{\#\{p \leq B\}}$ as $B \rightarrow \infty$

The Problem

$$\begin{array}{ccccc} X & \longrightarrow & \text{NS } X^{\text{al}} & \longrightarrow & \rho(X^{\text{al}}) & \in \{1, 2, \dots, 20\} \\ \downarrow & & \downarrow & & \updownarrow \text{???} & \\ X_p & \longrightarrow & \text{NS } X_p^{\text{al}} & \longrightarrow & \rho(X_p^{\text{al}}) & \in \{2, 4, \dots, 22\} \end{array}$$

Theorem (Charles)

For infinitely many p we have $\rho(X_p^{\text{al}}) = \min_q \rho(X_q^{\text{al}})$.

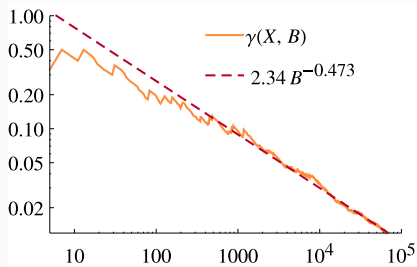
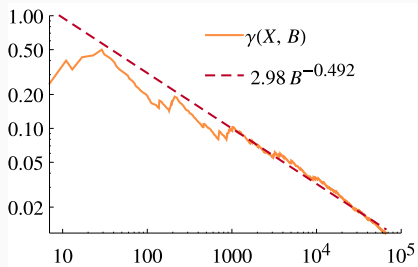
What can we say about:

- $\Pi_{\text{jump}}(X) := \{p : \rho(X_p^{\text{al}}) > \min_q \rho(X_q^{\text{al}})\}$
- $\gamma(X, B) := \frac{\#\{p \leq B : p \in \Pi_{\text{jump}}(X)\}}{\#\{p \leq B\}}$ as $B \rightarrow \infty$

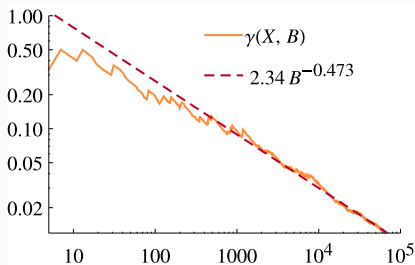
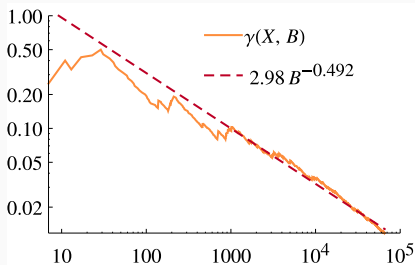
Let's do some numerical experiments!

Two generic K3 surfaces, $\rho(X^{\text{al}}) = 1$

Two generic K3 surfaces, $\rho(X^{\text{al}}) = 1$

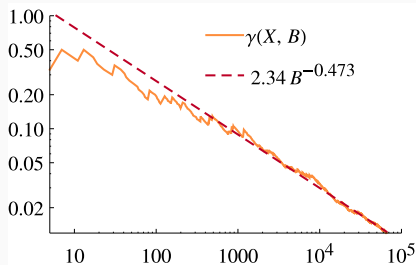
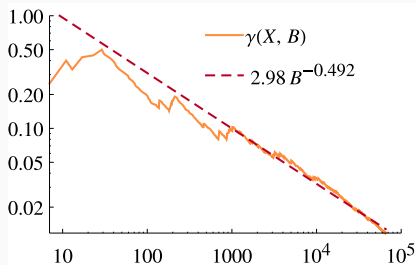


Two generic K3 surfaces, $\rho(X^{\text{al}}) = 1$



$$\gamma(X, B) \stackrel{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \rightarrow \infty$$

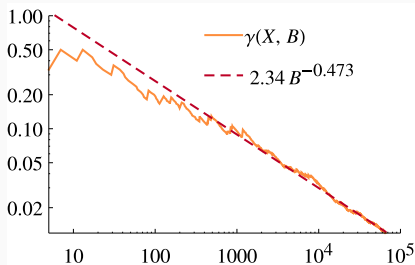
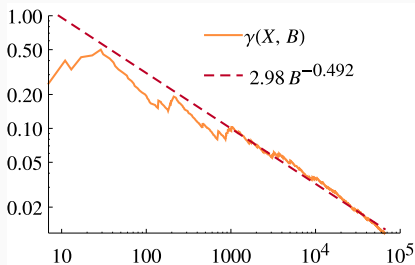
Two generic K3 surfaces, $\rho(X^{\text{al}}) = 1$



$$\gamma(X, B) \stackrel{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \rightarrow \infty$$

$$\implies \text{Prob}(p \in \Pi_{\text{jump}}(X)) \stackrel{?}{\sim} 1/\sqrt{p}$$

Two generic K3 surfaces, $\rho(X^{\text{al}}) = 1$



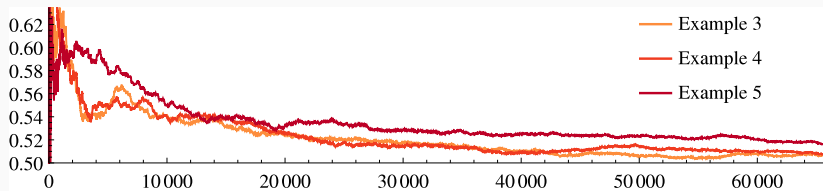
$$\gamma(X, B) \stackrel{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \rightarrow \infty$$

$$\implies \text{Prob}(p \in \Pi_{\text{jump}}(X)) \stackrel{?}{\sim} 1/\sqrt{p}$$

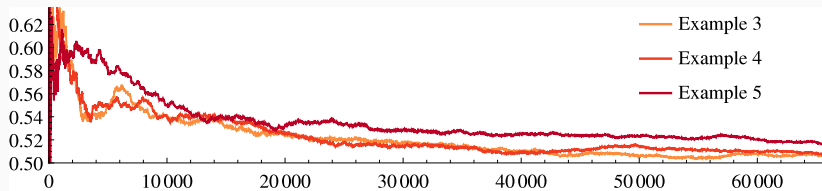
Why?

Three K3 surfaces with $\rho(X^{\text{al}}) = 2$

Three K3 surfaces with $\rho(X^{\text{al}}) = 2$

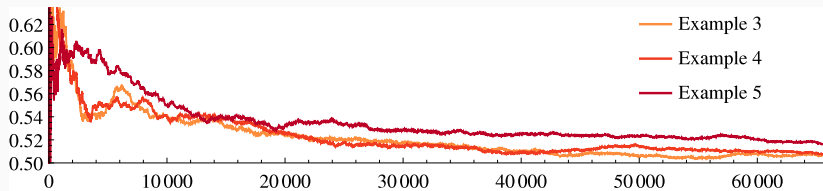


Three K3 surfaces with $\rho(X^{\text{al}}) = 2$



No obvious trend...

Three K3 surfaces with $\rho(X^{\text{al}}) = 2$



No obvious trend...

Could it be related to some integer being a square modulo p ?

We can explain the 1/2

Theorem (C, C-Eisenhans-Jahnel)

If $\rho(X^{\text{al}}) = \min_q \rho(X_p^{\text{al}})$, then there is a $d_X \in \mathbb{Z}$ such that:

$$\left\{ p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X}) \right\} \subset \Pi_{\text{jump}}(X).$$

In general, d_X is not a square.

We can explain the $1/2$

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X^{\text{al}}) = \min_q \rho(X_p^{\text{al}})$, then there is a $d_X \in \mathbb{Z}$ such that:

$$\left\{ p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X}) \right\} \subset \Pi_{\text{jump}}(X).$$

In general, d_X is not a square.

Corollary

If d_X is not a square:

- $\liminf_{B \rightarrow \infty} \gamma(X, B) \geq 1/2$
- X^{al} has infinitely many rational curves.

We can explain the $1/2$

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X^{\text{al}}) = \min_q \rho(X_p^{\text{al}})$, then there is a $d_X \in \mathbb{Z}$ such that:

$$\left\{ p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X}) \right\} \subset \Pi_{\text{jump}}(X).$$

In general, d_X is not a square.

Corollary

If d_X is not a square:

- $\liminf_{B \rightarrow \infty} \gamma(X, B) \geq 1/2$
- X^{al} has infinitely many rational curves.

$D_3 = -1 \cdot 5 \cdot 151 \cdot 22490817357414371041 \cdot 3873084974301493372336663588079962607808750567408509842132769703432789353$

$D_4 = 53 \cdot 2624174618795407 \cdot 512854561846964817139494202072778341 \cdot 1215218370089028769076718102126921744353362873 \cdot 68$

$D_5 = -1 \cdot 47 \cdot 3109 \cdot 4969 \cdot 14857095849982608071 \cdot 445410277660928347762586764331874432202584688016149 \cdot 65865270852$

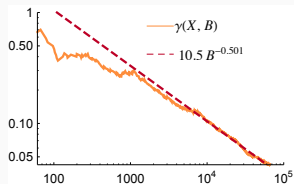
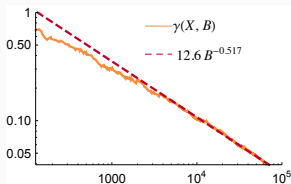
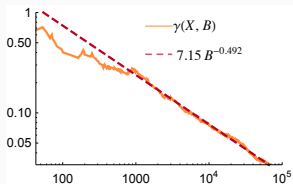
Experimental data for $\rho(X^{\text{al}}) = 2$ (again)

What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\text{jump}}(X)$?

Experimental data for $\rho(X^{\text{al}}) = 2$ (again)

What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\text{jump}}(X)$?

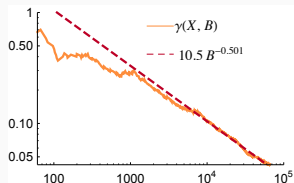
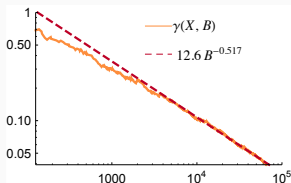
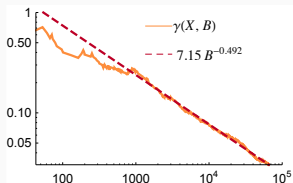
$$\gamma\left(X_{\mathbb{Q}(\sqrt{d_X})}, B\right) \stackrel{?}{\sim} \frac{C}{\sqrt{B}}, \quad B \rightarrow \infty$$



Experimental data for $\rho(X^{\text{al}}) = 2$ (again)

What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\text{jump}}(X)$?

$$\gamma\left(X_{\mathbb{Q}(\sqrt{d_X})}, B\right) \stackrel{?}{\sim} \frac{C}{\sqrt{B}}, \quad B \rightarrow \infty$$



$$\text{Prob}(p \in \Pi_{\text{jump}}(X)) = \begin{cases} 1 & \text{if } d_X \text{ is not a square modulo } p \\ \sim \frac{1}{\sqrt{p}} & \text{otherwise} \end{cases}$$

Why!?!?